РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 449 360** (13) **C1**

(51) МПК
G06F 21/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2011111600/08, 28.03.2011**

(24) Дата начала отсчета срока действия патента:
28.03.2011

Приоритет(ы):
(22) Дата подачи заявки: **28.03.2011**

(45) Опубликовано: **27.04.2012** Бюл. № **12**

(56) Список документов, цитированных в отчете о поиске: **RU 80037 U1, 20.01.2009. RU 2377639 C2, 27.12.2009. US 7743419 B1, 22.06.2010. WO 2010024606 A2, 04.03.2010.**

Адрес для переписки:
123060, Москва, 1-й Волоколамский пр-д, 10, корп.1, ЗАО Лаборатория Касперского, отдел по управлению интеллектуальной собственностью, Н.В. Кащенко

(72) Автор(ы):
Духвалов Андрей Петрович (RU)

(73) Патентообладатель(и):
Закрытое акционерное общество "Лаборатория Касперского" (RU)

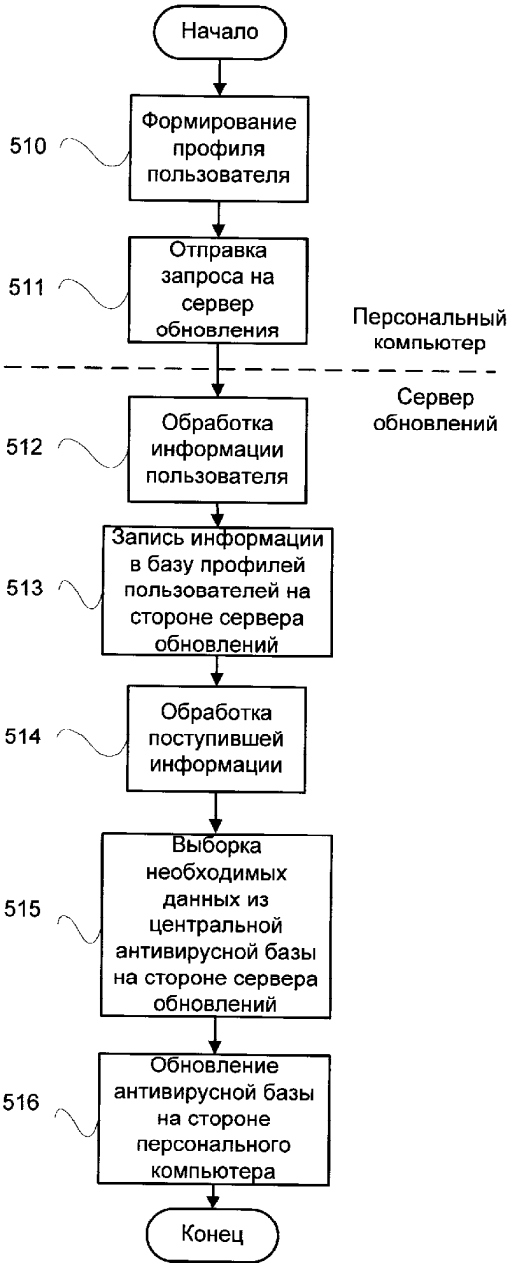
(54) СИСТЕМА И СПОСОБ ФОРМИРОВАНИЯ АНТИВИРУСНЫХ БАЗ В СООТВЕТСТВИИ С ПАРАМЕТРАМИ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА

(57) Реферат:

Данное изобретение относится к системам и способам антивирусной защиты и, более конкретно, к системам и способам формирования антивирусных баз данных в зависимости от параметров персонального компьютера. Технический результат заключается в оптимизации антивирусной базы данных, что достигается за счет динамического формирования базы данных в соответствии с параметрами персонального компьютера. При формировании антивирусных баз учитывается ряд параметров персональных компьютеров, таких как версия операционной системы, местоположения клиента и т.д. В зависимости от этих параметров формируются антивирусные базы, которые содержат только необходимую информацию для определенных пользователей. За счет того, что антивирусные базы содержат только необходимые данные, а не все имеющиеся данные, их размер уменьшается. 2 н. и 9 з.п. ф-лы, 6 ил.

RU 2449360 C1

RU 2449360 C1



Фиг. 5

RU 2449360 C1

RUSSIAN FEDERATION

(19) **RU** (11) **2 449 360** (13) **C1**

(51) Int. Cl.
G06F 21/00 (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2011111600/08, 28.03.2011**

(24) Effective date for property rights:
28.03.2011

Priority:
(22) Date of filing: **28.03.2011**

(45) Date of publication: **27.04.2012 Bull. 12**

Mail address:
123060, Moskva, 1-j Volokolamskij pr-d, 10, korp.1, ZAO Laboratorija Kasperskogo, otdel po upravleniju intellektual'noj sobstvennost'ju, N.V. Kashchenko

(72) Inventor(s):
Dukhvalov Andrej Petrovich (RU)

(73) Proprietor(s):
Zakrytoe aktsionernoe obshchestvo "Laboratorija Kasperskogo" (RU)

(54) SYSTEM AND METHOD FOR CREATING ANTIVIRUS DATABASES IN ACCORDANCE WITH PERSONAL COMPUTER PARAMETERS

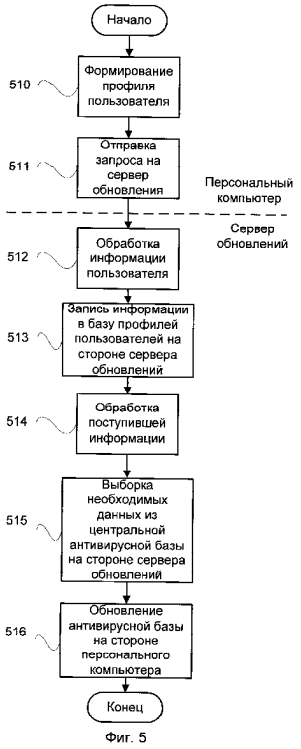
(57) Abstract:

FIELD: information technology.

SUBSTANCE: method is realised via dynamic creation of databases in accordance with personal computer parameters. When creating antivirus databases, several parameters of personal computers are considered, such as the operating system version, location of the client etc. Depending on these parameters, antivirus databases which contain only the necessary information for specific users are created. The size of the antivirus bases is therefore smaller owing to that the antivirus databases contain only the necessary data and not all available data.

EFFECT: optimisation of antivirus databases.

11 cl, 6 dwg



Фиг. 5

RU 2449360 C1

RU 2449360 C1

Область техники

Данное изобретение относится к антивирусным системам и, более конкретно, к системам и способам формирования антивирусных баз данных в зависимости от параметров персонального компьютера.

Уровень техники

В современном мире компьютерная техника получает все большую распространенность. Она становится доступней, мобильней, функциональней, а пользователи становятся опытнее в работе с компьютерной техникой. Такой высокий уровень развития может нести в себе также ряд угроз, связанных, например, со слабым уровнем защищенности цифровых данных.

Безопасность данных на персональных компьютерах (ПК), мобильной технике, промышленных компьютерах является актуальной проблемой. Каждый день появляется большое количество новых вредоносных приложений, способных стать причиной компьютерных сбоев, потери и кражи персональных данных. Многие вредоносные приложения модифицируются для того, чтобы их было сложнее обнаружить. Для сохранения антивирусной безопасности на высоком уровне производители антивирусных систем вынуждены постоянно выполнять пополнение антивирусных баз данных, которые используются при поиске вирусов.

Современные антивирусные базы содержат информацию разных типов: сигнатуры вредоносных объектов, в том числе и сигнатуры поведения, черные списки контрольных сумм, черные списки Интернет-сайтов, исполняемый код алгоритмов распаковки и эвристического анализа данных, информацию для устранения найденных угроз и т.п. Кроме того, антивирусные базы могут содержать необходимый код для обновления компонент антивирусной системы, таким образом, с помощью антивирусных баз возможно производить не только пополнение баз сигнатур, но и обновлять саму антивирусную систему.

Данные, содержащиеся в антивирусных базах, могут быть представлены по-разному. Представление данных в антивирусных базах напрямую зависит от антивирусной системы, в которой они используются. Форма и представление данных выбирается, исходя из ряда критериев, в число которых входит простота обновления, удобство работы, размер и т.д. Данные могут быть представлены в виде множества файлов, имеющих различные форматы, например формат динамических библиотек (Dynamic link library - DLL), XML-файлов или могут быть представлены в виде других форматов, в том числе форматов, применяющихся в конкретной антивирусной системе.

В настоящее время антивирусные базы содержат большое количество разнообразной информации, объем которой непрерывно увеличивается. Процесс увеличения антивирусных баз можно легко объяснить тем, что каждый день появляются новые вредоносные объекты, информация о которых попадает в антивирусные базы данных. Поскольку вредоносных объектов становится только больше, то и базы, содержащие информацию о таких объектах, увеличиваются в размере и становятся менее удобными для частого обновления.

Тенденция увеличения объема антивирусных баз данных является проблемой, которая уже стоит перед производителями антивирусных систем. Описываемое изобретение позволяет решить данную проблему и сделать антивирусные базы более удобными и мобильными.

В настоящее время известны системы обновления программных приложений с учетом различных параметров, описанные в заявках WO 2010024606 A2, KR

2009111152 A.

В заявке WO 2010024606 A2 рассматривается система и метод, предназначенные для подборки баз данных для компьютеров с учетом использующейся операционной системы и версии антивирусной программы.

В заявке KR 2009111152 A описывается система обновления антивирусных систем. Система основывается на классификации файлов, которые требуется проверить, составлении по результатам списка необходимых обновлений и загрузке обновлений.

Описываемая технология отличается от указанных, она предполагает автоматическое формирование баз по ряду параметров, список которых в общем случае не ограничен. Также антивирусная база формируется не только с учетом ее использования для проверки файлов, но с учетом ее использования при обеспечении комплексной защиты, необходимой конкретному пользователю.

Описываемая технология связана с ранее запатентованной технологией, описанной в патенте US 7743419, которая применяется для обнаружения и предотвращения эпидемий компьютерных вирусов. Технология основана на получении информации от персональных компьютеров и ее анализе с целью обнаружения эпидемий, их прогнозирования и предотвращения.

Анализ предшествующего уровня техники и возможностей, которые появляются при комбинировании их в одной системе, позволяют получить новый результат, а именно систему и способ динамического формирования антивирусных баз в соответствии с параметрами персонального компьютера без снижения уровня обнаружения вредоносных объектов антивирусной системой, использующей такие антивирусные базы.

Сущность изобретения

Технический результат настоящего изобретения заключается в оптимизации антивирусной базы данных для каждого персонального компьютера, что достигается за счет формирования базы данных в соответствии с параметрами персонального компьютера.

Настоящее изобретение представляет собой систему и способ формирования антивирусных баз в соответствии с параметрами персонального компьютера. Система формирования антивирусных баз, включающая сервер обновлений, связанный, по меньшей мере, с одним персональным компьютером, при этом персональный компьютер включает:

А) антивирусное средство, связанное со следующими средствами:

- антивирусной базой данных на стороне персонального компьютера,
- жестким диском персонального компьютера и
- средством формирования профиля пользователя на стороне персонального компьютера,

при этом антивирусное средство предназначено для проведения антивирусной проверки данных, хранящихся на жестком диске персонального компьютера, используя для проверки антивирусную базу данных на стороне персонального компьютера, а также для передачи информации об обнаруженных в результате антивирусной проверки вредоносных объектах на средство формирования профиля пользователя на стороне персонального компьютера;

Б) упомянутое средство формирования профиля пользователя на стороне персонального компьютера, связанное со следующими средствами:

- антивирусной базой данных на стороне персонального компьютера,
- жестким диском персонального компьютера и

- средством формирования запросов на стороне персонального компьютера,

при этом средство формирования профиля пользователя на стороне персонального компьютера предназначено для сбора параметров персонального компьютера, получаемых от антивирусной базы данных на стороне персонального компьютера, жесткого диска персонального компьютера и антивирусного средства на стороне персонального компьютера и отправки собранных параметров на средство формирования запросов на стороне персонального компьютера;

В) упомянутое средство формирования запросов на стороне персонального компьютера, связанное со средством обработки запросов на стороне сервера обновлений, предназначено для отправки параметров персонального компьютера, полученных от средства формирования профиля пользователя на стороне персонального компьютера, на средство обработки запросов на стороне сервера обновлений;

Г) средство обновления на стороне персонального компьютера, связанное со средством обновления на стороне сервера обновлений и антивирусной базой данных на стороне персонального компьютера, при этом средство обновления на стороне персонального компьютера выполнено с возможностью получения обновленной версии антивирусной базы данных от средства обновления на стороне сервера обновлений и предназначено для обновления антивирусной базы данных на стороне персонального компьютера;

Д) антивирусную базу данных на стороне персонального компьютера, содержащую данные, сформированные сервером обновлений для данного персонального компьютера по полученным параметрам персонального компьютера;

Е) жесткий диск персонального компьютера, содержащий, по меньшей мере, операционную систему и данные пользователя;

при этом сервер обновлений включает:

I) средство обработки запросов на стороне сервера обновлений, связанное со средством обработки данных на стороне сервера обновлений, при этом средство обработки запросов на стороне сервера обновлений выполнено с возможностью получения параметров, по меньшей мере, одного персонального компьютера от средства формирования запросов на стороне персонального компьютера и предназначено для сообщения средству обработки данных на стороне сервера обновлений о поступлении новых параметров, по меньшей мере, от одного персонального компьютера;

II) упомянутое средство обработки данных на стороне сервера обновлений, связанное со средством выборки данных на стороне сервера обновлений, при этом средство обработки данных на стороне сервера обновлений выполнено с возможностью проведения анализа поступивших параметров, по меньшей мере, от одного персонального компьютера, а также предназначено для формирования и передачи на средство выборки данных на стороне сервера обновлений требований к новой антивирусной базе по результатам анализа поступивших параметров;

III) упомянутое средство выборки данных на стороне сервера обновлений, связанное с:

- центральной антивирусной базой данных на стороне сервера обновлений;

- средством обновления на стороне сервера обновлений;

при этом средство выборки данных на стороне сервера обновлений предназначено для получения требований от средства обработки данных на стороне сервера обновлений и подготовки данных путем выборки данных, соответствующих

полученным требованиям, из центральной антивирусной базы данных на стороне сервера обновлений, также средство выборки данных на стороне сервера обновлений выполнено с возможностью передачи подготовленных данных средству обновления на стороне сервера обновлений;

IV) упомянутое средство обновления на стороне сервера обновлений выполнено с возможностью получения от средства выборки данных на стороне сервера обновлений подготовленных данных из центральной антивирусной базы данных на стороне сервера обновлений, а также предназначено для создания обновленной версии антивирусной базы данных и отправки обновленной версии антивирусной базы данных на средство обновления на стороне персонального компьютера;

V) упомянутую центральную антивирусную базу на стороне сервера обновлений, содержащую набор данных, необходимых для обнаружения вредоносных объектов.

В частном варианте исполнения упомянутая система дополнительно содержит базу профилей пользователей на стороне сервера обновлений, связанную со средством обработки запросов на стороне сервера обновлений и со средством обработки данных на стороне сервера обновлений, при этом база профилей пользователя на стороне сервера обновлений содержит параметры, по меньшей мере, одного персонального компьютера.

В частном варианте исполнения средство обработки запросов на стороне сервера обновлений дополнительно предназначено для помещения в базу профилей пользователей на стороне сервера обновлений параметры, по меньшей мере, одного персонального компьютера.

В частном варианте исполнения средство обработки данных на стороне сервера обновлений дополнительно предназначено для формирования требований к обновленной версии антивирусной базы на основе анализа параметров, находящихся в базе профилей пользователя на стороне сервера обновлений.

В частном варианте исполнения упомянутая система дополнительно содержит средство принудительного обновления на стороне сервера обновлений, связанное со следующими средствами:

- центральной антивирусной базой данных на стороне сервера обновлений;
- средством обработки данных на стороне сервера обновлений;

при этом средство принудительного обновления на стороне сервера обновлений предназначено для внеочередного запуска средства обработки данных на стороне сервера обновлений с целью принудительного обновления антивирусной базы данных на стороне персонального компьютера после обновления центральной антивирусной базы данных на стороне сервера обновлений.

В частном варианте исполнения параметры персонального компьютера включают, по меньшей мере, следующую информацию:

- местоположение персонального компьютера;
- версию операционной системы;
- локаль;
- информацию о программном обеспечении;
- версию антивирусного средства;
- версию антивирусной базы;
- статистику по посещаемым сайтам;
- статистику по обнаруженным объектам.

В частном варианте исполнения средство формирования профиля пользователя на стороне персонального компьютера настраивается для получения только части

данных антивирусной базы.

Способ формирования антивирусных баз в соответствии с параметрами персонального компьютера, выполняющийся на компьютере, заключается в том, что:

а) собирают параметры персонального компьютера при помощи средства формирования профиля пользователя на стороне персонального компьютера, получаемые от антивирусной базы данных на стороне персонального компьютера, жесткого диска персонального компьютера и антивирусного средства на стороне персонального компьютера;

б) отправляют параметры персонального компьютера, полученные от средства формирования профиля пользователя на стороне персонального компьютера, средством формирования запросов на стороне персонального компьютера на средство обработки запросов на стороне сервера обновлений;

в) получают параметры, по меньшей мере, одного персонального компьютера от средства формирования запросов на стороне персонального компьютера;

г) проводят средством обработки данных на стороне сервера обновлений анализ параметров, по меньшей мере, одного персонального компьютера, полученных от средства обработки запросов на стороне сервера обновлений, а также формируют и передают на средство выборки данных на стороне сервера обновлений требования к новой антивирусной базе по результатам анализа полученных параметров;

д) подготавливают данные путем выборки данных, соответствующих полученным требованиям, из центральной антивирусной базы данных на стороне сервера обновлений при помощи средства выборки данных на стороне сервера обновлений, также передают подготовленные данные средству обновления на стороне сервера обновлений;

е) получают подготовленные данные средством обновления на стороне сервера обновлений из центральной антивирусной базы данных на стороне сервера обновлений от средства выборки данных на стороне сервера обновлений, создают обновленную версию антивирусной базы данных и отправляют обновленную версию антивирусной базы данных на средство обновления на стороне персонального компьютера;

ж) получают обновленную версию антивирусной базы данных от средства обновления на стороне сервера обновлений и обновляют антивирусную базу данных на стороне персонального компьютера при помощи средства обновления на стороне персонального компьютера.

В частном варианте исполнения дополнительно вносят полученные параметры в базу профилей пользователей на стороне сервера обновлений средством обработки запросов на стороне сервера обновлений, а также сообщают средству обработки данных на стороне сервера обновлений о поступлении новых параметров, по меньшей мере, от одного персонального компьютера.

В частном варианте исполнения производят внеочередной запуск средства обработки данных на стороне сервера обновлений с целью принудительного обновления антивирусной базы данных на стороне персонального компьютера после обновления центральной антивирусной базы данных на стороне сервера обновлений при помощи средства принудительного обновления на стороне сервера обновлений.

В частном варианте исполнения средство формирования профиля пользователя на стороне персонального компьютера настраивают для получения только части

данных антивирусной базы.

Краткое описание чертежей

Дополнительные цели, признаки и преимущества настоящего изобретения будут очевидны из прочтения последующего описания осуществления изобретения со ссылкой на прилагаемые чертежи, на которых:

Фиг.1 показывает схему распределения персональных компьютеров пользователей.

Фиг.2 изображает часть системы на стороне персонального компьютера пользователя.

Фиг.3 показывает часть системы на стороне сервера обновлений.

Фиг.4 иллюстрирует базу профилей пользователей с содержащейся в ней информацией.

Фиг.5 показывает алгоритм работы системы динамического формирования антивирусных баз.

На Фиг.6 показана компьютерная система, на которой может быть реализовано описанное изобретение.

Хотя изобретение может иметь различные модификации и альтернативные формы, характерные признаки, показанные в качестве примера на чертежах, будут описаны подробно. Следует понимать, однако, что цель описания заключается не в ограничении изобретения конкретным его воплощением. Наоборот, целью описания является охват всех изменений, модификаций, входящих в рамки данного изобретения, как это определено приложенной формулой.

Описание вариантов осуществления изобретения

Объекты и признаки настоящего изобретения, способы для достижения этих объектов и признаков станут очевидными посредством отсылки к примерным вариантам осуществления. Однако настоящее изобретение не ограничивается примерными вариантами осуществления, раскрытыми ниже, оно может воплощаться в различных видах. Сущность, приведенная в описании, является ничем иным, как конкретными деталями для помощи специалисту в области техники в исчерпывающем понимании изобретения. Настоящее изобретение определяется только в объеме приложенной формулы.

На данный момент существует большое многообразие вредоносных приложений, в том числе компьютерных вирусов, троянских программ, сетевых червей и т.д. Все известные вредоносные приложения, а также многие неизвестные, могут быть обнаружены антивирусной системой с помощью антивирусных баз. Однако зачастую пользователю, на персональном компьютере которого имеется антивирусная система, незачем иметь полную антивирусную базу, включающую описание всех известных вредоносных объектов, с многими из которых пользователь никогда не столкнется. Например, не имеет смысла обновлять антивирусную базу черным списком Интернет-сайтов одной доменной зоны, если пользователь работает в совершенно другой доменной зоне и не посещает интернет-сайты первой доменной зоны.

Можно привести другой пример. На персональных компьютерах пользователей установлены разные версии операционных систем (ОС). Для разных версий операционных систем имеются свои виды угроз заражения вредоносными приложениями, поэтому использование антивирусных баз, созданных для определенной операционной системы, было бы более эффективным решением, чем использование универсальной антивирусной базы, которая подходит для всех видов

угроз, часть из которых не возникнет в данной операционной системе.

Таким образом, если выделить для пользователей характерные параметры, которые будут влиять на то, что будут содержать антивирусные базы для каждого пользователя, можно составить антивирусные базы, оптимально подходящими для каждого пользователя. Создание антивирусных баз для отдельных пользователей не повлечет снижение уровня защищенности от вредоносных объектов, поскольку базы формируются динамически, то есть при изменении параметров компьютера пользователя или при появлении новых для пользователя видов угроз антивирусная база будет изменена в соответствии появившимися изменениями. При этом сама процедура обновления становится более удобной из-за того, что не приходится загружать большой объем данных при обновлении. Также антивирусная система, работающая с антивирусной базой, небольшой по размеру, более эффективно проводит поиск вредоносных объектов, используя меньшие ресурсы компьютерной системы.

На Фиг.1 показана схема взаимодействия персональных компьютеров пользователей с сервером обновлений.

На Фиг.1 показаны персональные компьютеры пользователей 120-128, которые обладают рядом параметров, влияющих на формирование антивирусных баз для каждого пользователя. Параметры, влияющие на формирование баз, будут описаны далее.

Каждый персональный компьютер 120-128 имеет свою антивирусную базу. Если несколько компьютеров имеют одинаковые параметры, то антивирусные базы для таких компьютеров будут содержать одинаковые данные. Антивирусные базы для компьютеров, имеющих неодинаковые параметры, отличаются, но могут иметь общие данные.

Все персональные компьютеры имеют доступ к серверу обновлений 110, на который стекается информация от всех компьютеров пользователей. Подобный доступ может обеспечиваться, например, с использованием технологии Kaspersky Security Network (KSN), позволяющей в реальном режиме времени собирать информацию от компьютеров пользователей о существующих угрозах, а также эффективно выявлять неизвестные угрозы и их источники, оперативно защищая от них пользователей.

Доступ осуществляется при помощи сетевых соединений посредством сети Интернет 130. Сервер обновлений 110 формирует антивирусные базы для каждого пользователя, применяя для этого центральную антивирусную базу данных 111. От параметров персонального компьютера будет зависеть состав данных антивирусной базы. Сервер обновлений может изменять антивирусную базу при изменении параметров ПК пользователя.

Центральная антивирусная база 111 содержит данные, которые необходимы для работы антивирусной системы на персональном компьютере пользователя с любыми параметрами. При этом центральная антивирусная база 111 имеет больший размер, по сравнению с антивирусными базами пользователей, поскольку содержит большинство известных на текущий момент записей о вредоносных объектах.

Для лучшего понимания системы динамического формирования антивирусных баз в соответствии с параметрами персонального компьютера необходимо рассмотреть более подробно каждый модуль системы.

На Фиг.2 изображена часть системы на стороне персонального компьютера пользователя. В одном из вариантов осуществления персональный компьютер

пользователя 210 включает следующие средства: антивирусное средство на стороне персонального компьютера 211, производящее поиск вредоносных объектов среди данных, хранящихся на жестком диске 212 персонального компьютера. Антивирусное средство на стороне персонального компьютера 211 использует для выполнения своих задач антивирусную базу данных на стороне персонального компьютера 216. Например, на жестком диске 212 хранится операционная система, веб-браузер, почтовый клиент и другие файлы пользователя. Персональный компьютер пользователя 210 содержит также средство формирования профиля пользователя на стороне персонального компьютера 213. Данное средство собирает необходимые параметры для формирования профиля пользователя. Достаточный набор параметров содержат, по меньшей мере, следующую информацию:

- идентификатор пользователя (уникальный номер);
- местоположение пользователя (пользователи разделены по местоположению, в качестве местоположения могут выступать географические объекты, например, отдельные страны или группы стран, объединенные в регионы);
- информацию о компьютере пользователя (версия ОС; локаль - набор параметров, включая набор символов, язык пользователя, страну, часовой пояс, а также другие предустановки; тип веб-браузера; тип почтового клиента и т.д.);
- версию антивирусного средства;
- версию антивирусных баз;
- статистику по посещаемым сайтам;
- статистику по обнаруженным объектам.

В качестве параметра персонального компьютера может выступать список используемых пользователем программных приложений, которые также могут быть использованы вредоносными объектами при получении доступа к данным пользователя. Подобного рода информация должна учитываться, чтобы сформированные антивирусные базы оптимально подходили для каждого пользователя с учетом используемых программных приложений.

Информация о компьютере пользователя необходима серверу обновлений в качестве критерия при формировании антивирусных баз. Например, если компьютеры имеют одно местоположение, у компьютеров одинаковая операционная система, пользователи используют один и тот же веб-браузер для просмотра интернет-страниц, применяются одинаковые почтовые клиенты и т.д., то антивирусные базы, которые будут использоваться на таких компьютерах, будут идентичными. Состав антивирусной базы на стороне персонального компьютера 216 в свою очередь будет зависеть от каждого параметра персонального компьютера пользователя 210.

Приведенный список параметров не является строго фиксированным, он может дополняться и другими параметрами. Основная задача при этом получить такой набор параметров, который позволил бы составить оптимальные антивирусные базы для каждого персонального компьютера. То есть такие антивирусные базы, которые бы обеспечили максимальный уровень защиты ПК пользователей и в то же время имели меньший размер. В таком случае достигается технический результат изобретения, а именно создание оптимальных антивирусных баз 216 за счет динамического формирования базы данных в соответствии с параметрами персонального компьютера пользователя 210.

Система имеет дополнительные настройки. Например, если персональный компьютер пользователя используется в качестве почтового сервера, то средство

формирования профиля пользователя на стороне персонального компьютера 213 может быть настроено так, что персональный компьютер будет получать только ту часть антивирусной базы, которая нужна для поиска вирусов и спама в почтовых сообщениях. Но антивирусная база на стороне персонального компьютера 216 не будет содержать ту часть, которая используется для поиска вирусов на загружаемых веб-страницах, размер антивирусной базы на стороне персонального компьютера 216, соответственно, уменьшится.

Возможен случай, когда, в силу ограниченности ресурсов (например, при ограничении полосы пропускания интернет-соединения), система настраивает средство формирования профиля пользователя на стороне персонального компьютера 213 так, что будет получать, например, только часть сигнатур, которые соответствуют самым распространенным вредоносным объектам. В таком варианте уровень защиты от вредоносных объектов снизится незначительно, но объем антивирусной базы на стороне персонального компьютера 216 будет уменьшен.

Средство формирования профиля пользователя на стороне персонального компьютера 213 подготавливает всю необходимую информацию для отправки на сервер обновлений.

При первичной регистрации пользователя 210 на сервере обновлений 310, персональный компьютер пользователя 210 производит сбор необходимых для регистрации данных. Для этого он обращается к жесткому диску 212 и получает данные о программных приложениях и операционной системе; к антивирусному средству на стороне персонального компьютера 211 для получения версии антивирусного средства; к антивирусной базе на стороне персонального компьютера 216 для получения информации о версии базы. После того, как вся необходимая информация получена, она передается от средства формирования профиля пользователя на стороне персонального компьютера 213 на средство формирования запросов на стороне персонального компьютера 214, которое отправляет запрос со всей информацией на сервер обновлений 310.

При первичной регистрации новый пользователь получает антивирусную базу, которая будет сформирована по тем данным, которые были предоставлены пользователем при первичной регистрации. При первичной регистрации нет возможности предоставить полный набор параметров для формирования оптимальной базы, однако со временем будет поступать новая информация, и антивирусная база для персонального компьютера пользователя будет модифицироваться. В конце пользователь будет иметь оптимальную для него антивирусную базу.

Если на персональном компьютере пользователя происходят изменения, например, было произведено обновление операционной системы, было установлено новое программное обеспечение и т.д., такие события фиксируются средством формирования профиля пользователя на стороне персонального компьютера 213 и передаются на сервер обновлений 310. Если такое событие произойдет, то сервер 310 обновит антивирусную базу пользователя, загрузив новые данные, которые актуальны для текущего набора параметров.

Помимо сбора информации об изменениях на персональном компьютере пользователя 210, средство формирования профиля пользователя на стороне персонального компьютера 213 получает информацию о найденных вредоносных объектах от антивирусного средства на стороне персонального компьютера 211 и передает эту информацию также на сервер обновлений 310, используя средство

формирования запросов на стороне персонального компьютера 214. На сервере обновлений 310 в одном из вариантов реализации происходит сбор статистики, которая учитывается при формировании антивирусных баз.

На персональном компьютере пользователя 210 также присутствует средство обновления на стороне персонального компьютера 215, которое служит для получения новой версии антивирусной базы от сервера 310 и обновления антивирусной базы на стороне персонального компьютера 216.

На Фиг.3 показана часть системы на стороне сервера обновлений.

Связь сервера обновлений 310 с персональными компьютерами пользователя осуществляется благодаря средству обработки запросов на стороне сервера обновлений 311. Средство обработки запросов на стороне сервера обновлений 311 принимает запросы, поступающие на сервер от персональных компьютеров, производит их обработку. В одном из вариантов осуществления средство обработки запросов на стороне сервера обновлений 311 вносит новые данные, содержащиеся в запросе, в базу профилей пользователей на стороне сервера обновлений 312. Также средство обработки запросов на стороне сервера обновлений 311 сообщает средству обработки данных на стороне сервера обновлений 313 о поступлении новых данных от пользователей. Если система не содержит базу профилей пользователей 312, то средство обработки запросов на стороне сервера обновлений 311 передает полученные данные непосредственно на средство обработки данных на стороне сервера обновлений 313.

База профилей пользователя на стороне сервера обновлений 312 содержит информацию о пользователях, она нужна для ускорения процесса анализа данных пользователя и не влияет на процесс формирования антивирусных баз. Поэтому в частных вариантах реализации база профилей пользователей на стороне сервера обновлений 312 может отсутствовать.

Информация, содержащаяся в базе профилей пользователей 312, описана на Фиг.4. Каждый пользователь имеет уникальный номер - идентификатор пользователя. В базе 312 хранится также вся информация, поступающая в запросах, а именно: местоположение пользователя; информация о компьютере пользователя; версия антивирусного средства; версия антивирусных баз; период накопления данных; статистика по посещаемым сайтам; статистика по обнаруженным объектам и т.д.

Средство обработки данных на стороне сервера обновлений 313 проводит обработку информации о персональном компьютере пользователя, в том числе проводит анализ данных по обнаруженным объектам. Такой анализ может проводиться с определенной периодичностью в случае планового проведения обновления антивирусных баз пользователей либо при поступлении запроса пользователя о внеочередном обновлении антивирусной базы.

Если антивирусная база пользователя требует обновления, то от персонального компьютера пользователя приходит соответствующий запрос, который прорабатывается средством обработки запросов на стороне сервера обновлений 311. После средство обработки данных на стороне сервера обновлений 313 проводит анализ данных из базы 312, и по результатам анализа базы профилей пользователей на стороне сервера обновлений 312 средство обработки данных 313 формирует требования к антивирусной базе для данного пользователя средству выборки данных на стороне сервера обновлений 314.

Если какой-то параметр персонального компьютера пользователя изменился, то

от него приходит запрос с указанием изменившегося параметра. Этот запрос обрабатывается средством обработки запросов на стороне сервера обновлений 311, изменившийся параметр заносится в базу 312 и средство обработки данных на стороне сервера обновлений 313 формирует новые требования в соответствии с полученными изменениями.

Средство выборки данных на стороне сервера обновлений 314 получает требования от средства 313, потом подготавливает необходимые данные, производя выборку из центральной антивирусной базы на стороне сервера обновлений 315, и передает их при помощи средства обновления на стороне сервера обновлений 316 на персональный компьютер пользователя 210. Средство обновления на стороне персонального компьютера 215 принимает данные и обновляет антивирусную базу на стороне персонального компьютера 216.

Вредоносные объекты периодически модифицируются, а также появляются новые вредоносные объекты, в связи с этим центральная антивирусная база на стороне сервера обновлений 315 также может изменяться и пополняться новыми данными, а старые и неактуальные данные из нее могут удаляться. Поэтому все изменения в центральной базе должны находить отражения в антивирусных базах на компьютерах пользователей. Для этого применяется средство принудительного обновления на стороне сервера обновлений 317, которое при обновлении центральной антивирусной базы на стороне сервера обновлений 315 передает уведомление об этом на средство обработки данных на стороне сервера обновлений 313, которое во внеочередном порядке начинает процесс анализа данных и формирования новых требований к антивирусным базам для отдельных ПК пользователей. Далее процесс обновления идет аналогично описанному выше процессу.

Далее будет описан алгоритм работы системы динамического формирования антивирусных баз в соответствии с параметрами персонального компьютера.

На Фиг.5 показан алгоритм работы системы динамического формирования антивирусных баз.

В системе на стороне персонального компьютера пользователя 210 возможно появление различных событий, например, обнаружение нового вредоносного объекта либо возникновение необходимости в плановом или экстренном обновлении антивирусной базы на стороне персонального компьютера 216, либо изменение параметров персонального компьютера пользователя, в том числе изменение состава программного обеспечения, установленного на персональном компьютере пользователя 210 и т.д. Все эти события собираются средством формирования профиля пользователя на стороне персонального компьютера 213. После чего модуль 213 на шаге 510 формирует профиль пользователя.

Когда профиль пользователя сформирован, информация о нем передается на средство формирования запросов на стороне персонального компьютера 214, которое отправляет информацию на сервер обновлений на шаге 511.

Запросы, которые формируются на персональных компьютерах пользователей, поступают на сервер обновлений, а именно на средство обработки запросов на стороне сервера обновлений 311, которое производит обработку информации, полученной от пользователя, на шаге 512. Если произошло изменение одного из параметров ПК пользователя, информация о таком событии отражается в базе профилей пользователей на стороне сервера обновлений 312 на шаге 513. При этом данный шаг отсутствует у систем, не использующих базу профилей пользователей на

стороне сервера обновлений 312. В таком случае информация, полученная от пользователей, передается сразу на средство обработки данных на стороне сервера обновлений 313.

Далее средство обработки данных на стороне сервера обновлений 313 производит анализ данных и формирует требования к антивирусной базе на шаге 514. Сформированные требования поступают на средство выборки данных на стороне сервера обновлений 314, и на шаге 515 производится извлечение данных из центральной антивирусной базы 315. Данные из центральной антивирусной базы на стороне сервера обновлений 315 отправляются на персональный компьютер пользователя 210 при помощи средства обновления на стороне сервера обновлений 316 на шаге 516, и антивирусная база пользователя на стороне персонального компьютера 216 обновляется средством обновления на стороне персонального компьютера 215.

На Фиг.6 показана компьютерная система, на которой может быть реализовано описанное изобретение в рамках данного варианта реализации.

На Фиг.6 представлен пример компьютерной системы 20, содержащей центральный процессор 21, системную память 22 и системную шину 23, которая содержит разные системные компоненты, в том числе память, связанную с центральным процессором 21. Системная шина 23 реализована, как любая известная из уровня техники шинная структура, содержащая в свою очередь память шины или контроллер памяти шины, периферийную шину и локальную шину, которая способна взаимодействовать с любой другой шинной архитектурой. Системная память содержит постоянное запоминающее устройство (ПЗУ) 24, память с произвольным доступом (ОЗУ) 25. Основная система ввода/вывода (BIOS) содержит основные процедуры, которые обеспечивают передачу информации между элементами персонального компьютера 20, например, в момент загрузки операционной системы с использованием ПЗУ 24.

Персональный компьютер 20 в свою очередь содержит жесткий диск 27 для чтения и записи данных, привод магнитных дисков 28 для чтения и записи на сменные магнитные диски 29 и оптический привод 30 для чтения и записи на сменные оптические диски 31, такие как CD-ROM, DVD-ROM и иные оптические носители информации. Жесткий диск 27, привод магнитных дисков 28, оптический привод 30 соединены с системной шиной 23 через интерфейс жесткого диска 32, интерфейс привода магнитных дисков 33 и интерфейс оптического привода 34 соответственно. Приводы и соответствующие компьютерные носители информации представляют собой энергонезависимые средства хранения компьютерных инструкций, структур данных, программных модулей и прочих данных персонального компьютера 20.

Настоящее описание раскрывает реализацию системы, которая использует жесткий диск, сменный магнитный диск 29 и сменный оптический диск 31, но следует понимать, что возможно применение иных типов компьютерных носителей информации, которые способны хранить данные в доступной для чтения компьютером форме (твердотельные накопители, флеш-карты памяти, цифровые диски, память с произвольным доступом (ОЗУ) и т.п.).

Компьютер 20 имеет файловую систему 36, где хранится записанная операционная система 35 и дополнительные программные приложения 37, другие программные модули 38 и программные данные 39. Пользователь имеет возможность вводить команды и информацию в персональный компьютер 20 посредством устройств ввода (клавиатуры 40, манипулятора «мышь» 42). Могут использоваться другие

устройства ввода (не отображены): микрофон, джойстик, игровая консоль, сканнер и т.п. Подобные устройства ввода по своему обычаю подключают к компьютерной системе 20 через последовательный порт 46, который в свою очередь подсоединен к системной шине, но могут быть подключены иным способом, например, при помощи параллельного порта, игрового порта или универсальной последовательной шины (USB). Монитор 47 или иной тип устройства отображения также подсоединен к системной шине 23 через интерфейс, такой как видеоадаптер 48. В дополнение к монитору 47, персональный компьютер может быть оснащен другими периферийными устройствами вывода (не отображены), например, колонки, принтер и т.п.

Персональный компьютер 20 способен работать в сетевом окружении, при этом используется сетевое соединение с другим или несколькими удаленными компьютерами 49. Удаленный компьютер (или компьютеры) 49 являются такими же персональными компьютерами или серверами, которые имеют большинство или все упомянутые элементы, отмеченные ранее при описании существа персонального компьютера 20, представленного на Фиг.6. В вычислительной сети могут присутствовать также и другие устройства, например, маршрутизаторы, сетевые станции, пиринговые устройства или иные сетевые узлы.

Сетевые соединения могут образовывать локальную вычислительную сеть (LAN) 51 и глобальную вычислительную сеть (WAN) 52. Такие сети применяются в корпоративных компьютерных сетях, внутренних сетях компаний и, как правило, имеют доступ к сети Интернет. В LAN- или WAN-сетях персональный компьютер 20 подключен к локальной сети 51 через сетевой адаптер или сетевой интерфейс 53. При использовании сетей персональный компьютер 20 может использовать модем 54 или иные средства обеспечения связи с глобальной вычислительной сетью 52, такой как Интернет. Модем 54, который является внутренним или внешним устройством, подключен к системной шине 23 посредством последовательного порта 46. Следует уточнить, что сетевые соединения являются лишь примерными, и не обязаны отображать точную конфигурацию сети, т.е. в действительности существуют иные способы установления соединения техническими средствами связи одного компьютера с другим.

В заключение следует отметить, что приведенные в описании сведения являются примерами, которые не ограничивают объем настоящего изобретения, определенного формулой. Специалисту в данной области становится понятным, что могут существовать и другие варианты осуществления настоящего изобретения, согласующиеся с сущностью и объемом настоящего изобретения.

Формула изобретения

1. Система формирования антивирусных баз, включающая сервер обновлений, связанный, по меньшей мере, с одним персональным компьютером, при этом персональный компьютер включает:

А) антивирусное средство, связанное со следующими средствами:

антивирусной базой данных на стороне персонального компьютера,

жестким диском персонального компьютера и

средством формирования профиля пользователя на стороне персонального компьютера,

при этом антивирусное средство предназначено для проведения антивирусной проверки данных, хранящихся на жестком диске персонального компьютера,

используя для проверки антивирусную базу данных на стороне персонального компьютера, а также для передачи информации об обнаруженных в результате антивирусной проверки вредоносных объектах на средство формирования профиля пользователя на стороне персонального компьютера;

Б) упомянутое средство формирования профиля пользователя на стороне персонального компьютера, связанное со следующими средствами:

антивирусной базой данных на стороне персонального компьютера,

жестким диском персонального компьютера и

средством формирования запросов на стороне персонального компьютера,

при этом средство формирования профиля пользователя на стороне персонального компьютера предназначено для сбора параметров персонального компьютера, получаемых от антивирусной базы данных на стороне персонального компьютера, жесткого диска персонального компьютера и антивирусного средства на стороне персонального компьютера, и отправки собранных параметров на средство формирования запросов на стороне персонального компьютера;

В) упомянутое средство формирования запросов на стороне персонального компьютера, связанное со средством обработки запросов на стороне сервера обновлений, предназначено для отправки параметров персонального компьютера, полученных от средства формирования профиля пользователя на стороне персонального компьютера, на средство обработки запросов на стороне сервера обновлений;

Г) средство обновления на стороне персонального компьютера, связанное со средством обновления на стороне сервера обновлений и антивирусной базой данных на стороне персонального компьютера, при этом средство обновления на стороне персонального компьютера выполнено с возможностью получения обновленной версии антивирусной базы данных от средства обновления на стороне сервера обновлений и предназначено для обновления антивирусной базы данных на стороне персонального компьютера;

Д) антивирусную базу данных на стороне персонального компьютера, содержащую данные, сформированные сервером обновлений для данного персонального компьютера по полученным параметрам персонального компьютера;

Е) жесткий диск персонального компьютера, содержащий, по меньшей мере, операционную систему и данные пользователя;

при этом сервер обновлений включает:

I) средство обработки запросов на стороне сервера обновлений, связанное со средством обработки данных на стороне сервера обновлений, при этом средство обработки запросов на стороне сервера обновлений выполнено с возможностью получения параметров, по меньшей мере, одного персонального компьютера от средства формирования запросов на стороне персонального компьютера и предназначено для сообщения средству обработки данных на стороне сервера обновлений о поступлении новых параметров, по меньшей мере, от одного персонального компьютера;

II) упомянутое средство обработки данных на стороне сервера обновлений, связанное со средством выборки данных на стороне сервера обновлений, при этом средство обработки данных на стороне сервера обновлений выполнено с возможностью проведения анализа поступивших параметров, по меньшей мере, от одного персонального компьютера, а также предназначено для формирования и передачи на средство выборки данных на стороне сервера обновлений требований к

новой антивирусной базе по результатам анализа поступивших параметров;

III) упомянутое средство выборки данных на стороне сервера обновлений, связанное с:

центральной антивирусной базой данных на стороне сервера обновлений;

средством обновления на стороне сервера обновлений;

при этом средство выборки данных на стороне сервера обновлений предназначено для получения требований от средства обработки данных на стороне сервера обновлений и подготовки данных путем выборки данных, соответствующих полученным требованиям, из центральной антивирусной базы данных на стороне сервера обновлений, также средство выборки данных на стороне сервера обновлений выполнено с возможностью передачи подготовленных данных средству обновления на стороне сервера обновлений;

IV) упомянутое средство обновления на стороне сервера обновлений выполнено с возможностью получения от средства выборки данных на стороне сервера обновлений подготовленных данных из центральной антивирусной базы данных на стороне сервера обновлений, а также предназначено для создания обновленной версии антивирусной базы данных и отправки обновленной версии антивирусной базы данных на средство обновления на стороне персонального компьютера;

V) упомянутую центральную антивирусную базу на стороне сервера обновлений, содержащую набор данных, необходимых для обнаружения вредоносных объектов.

2. Система по п.1, которая дополнительно содержит базу профилей пользователей на стороне сервера обновлений, связанную со средством обработки запросов на стороне сервера обновлений и со средством обработки данных на стороне сервера обновлений, при этом база профилей пользователя на стороне сервера обновлений содержит параметры, по меньшей мере, одного персонального компьютера.

3. Система по п.2, в которой средство обработки запросов на стороне сервера обновлений дополнительно предназначено для помещения в базу профилей пользователей на стороне сервера обновлений параметров, по меньшей мере, одного персонального компьютера.

4. Система по п.2, в которой средство обработки данных на стороне сервера обновлений дополнительно предназначено для формирования требований к обновленной версии антивирусной базы на основе анализа параметров, находящихся в базе профилей пользователя на стороне сервера обновлений.

5. Система по п.1, которая дополнительно содержит средство принудительного обновления на стороне сервера обновлений, связанное со следующими средствами:

центральной антивирусной базой данных на стороне сервера обновлений;

средством обработки данных на стороне сервера обновлений;

при этом средство принудительного обновления на стороне сервера обновлений предназначено для внеочередного запуска средства обработки данных на стороне сервера обновлений с целью принудительного обновления антивирусной базы данных на стороне персонального компьютера после обновления центральной антивирусной базы данных на стороне сервера обновлений.

6. Система по п.1, в которой параметры персонального компьютера включают, по меньшей мере, следующую информацию:

местоположение персонального компьютера;

версию операционной системы;

локаль;

информацию о программном обеспечении;

версию антивирусного средства;
версию антивирусной базы;
статистику по посещаемым сайтам;
статистику по обнаруженным объектам.

7. Система по п.1, в которой средство формирования профиля пользователя на стороне персонального компьютера настраивается для получения только части данных антивирусной базы.

8. Способ формирования антивирусных баз в соответствии с параметрами персонального компьютера, выполняющийся на компьютере, заключается в том, что:

а) собирают параметры персонального компьютера при помощи средства формирования профиля пользователя на стороне персонального компьютера, получаемые от антивирусной базы данных на стороне персонального компьютера, жесткого диска персонального компьютера и антивирусного средства на стороне персонального компьютера;

б) отправляют параметры персонального компьютера, полученные от средства формирования профиля пользователя на стороне персонального компьютера, средством формирования запросов на стороне персонального компьютера на средство обработки запросов на стороне сервера обновлений;

в) получают параметры, по меньшей мере, одного персонального компьютера от средства формирования запросов на стороне персонального компьютера;

г) проводят средством обработки данных на стороне сервера обновлений анализ параметров, по меньшей мере, одного персонального компьютера, полученных от средства обработки запросов на стороне сервера обновлений, а также формируют и передают на средство выборки данных на стороне сервера обновлений требования к новой антивирусной базе по результатам анализа полученных параметров;

д) подготавливают данные путем выборки данных, соответствующих полученным требованиям, из центральной антивирусной базы данных на стороне сервера обновлений при помощи средства выборки данных на стороне сервера обновлений, также передают подготовленные данные средству обновления на стороне сервера обновлений;

е) получают подготовленные данные средством обновления на стороне сервера обновлений из центральной антивирусной базы данных на стороне сервера обновлений от средства выборки данных на стороне сервера обновлений, создают обновленную версию антивирусной базы данных и отправляют обновленную версию антивирусной базы данных на средство обновления на стороне персонального компьютера;

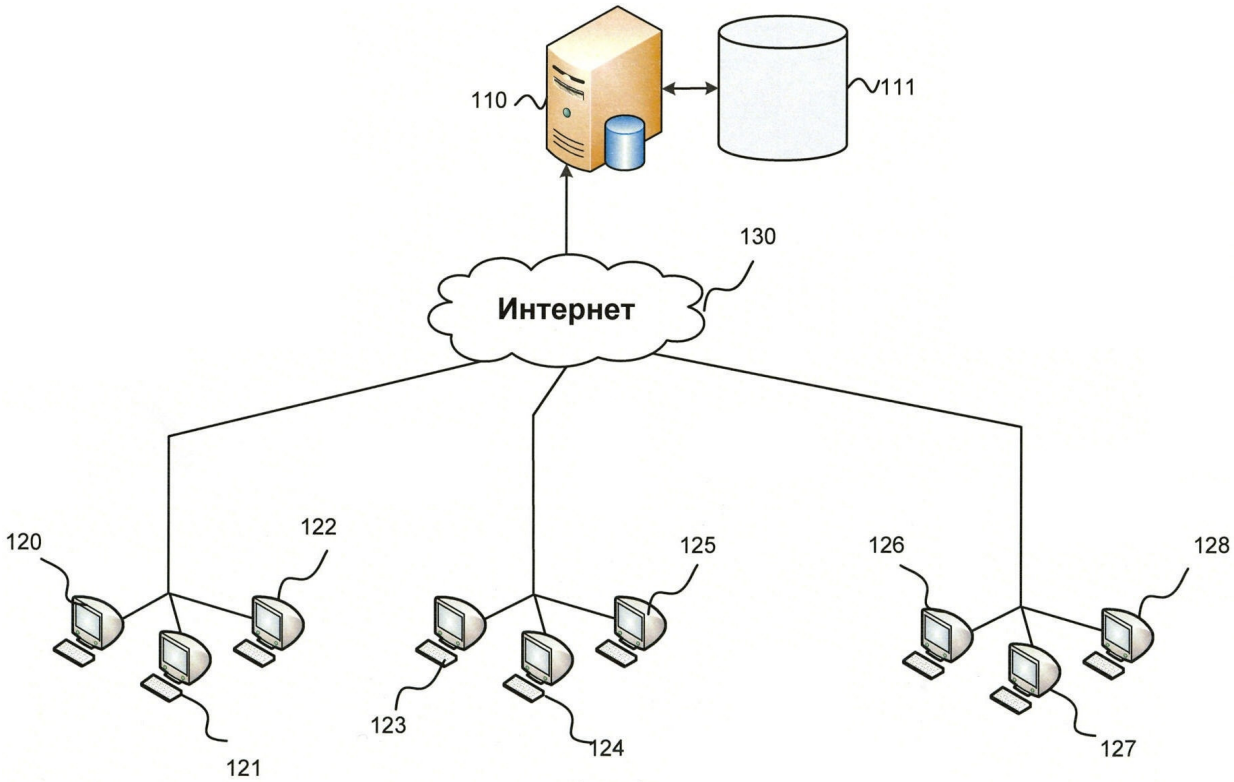
ж) получают обновленную версию антивирусной базы данных от средства обновления на стороне сервера обновлений и обновляют антивирусную базу данных на стороне персонального компьютера при помощи средства обновления на стороне персонального компьютера.

9. Способ по п.8, в котором дополнительно вносят полученные параметры в базу профилей пользователей на стороне сервера обновлений средством обработки запросов на стороне сервера обновлений, а также сообщают средству обработки данных на стороне сервера обновлений о поступлении новых параметров, по меньшей мере, от одного персонального компьютера.

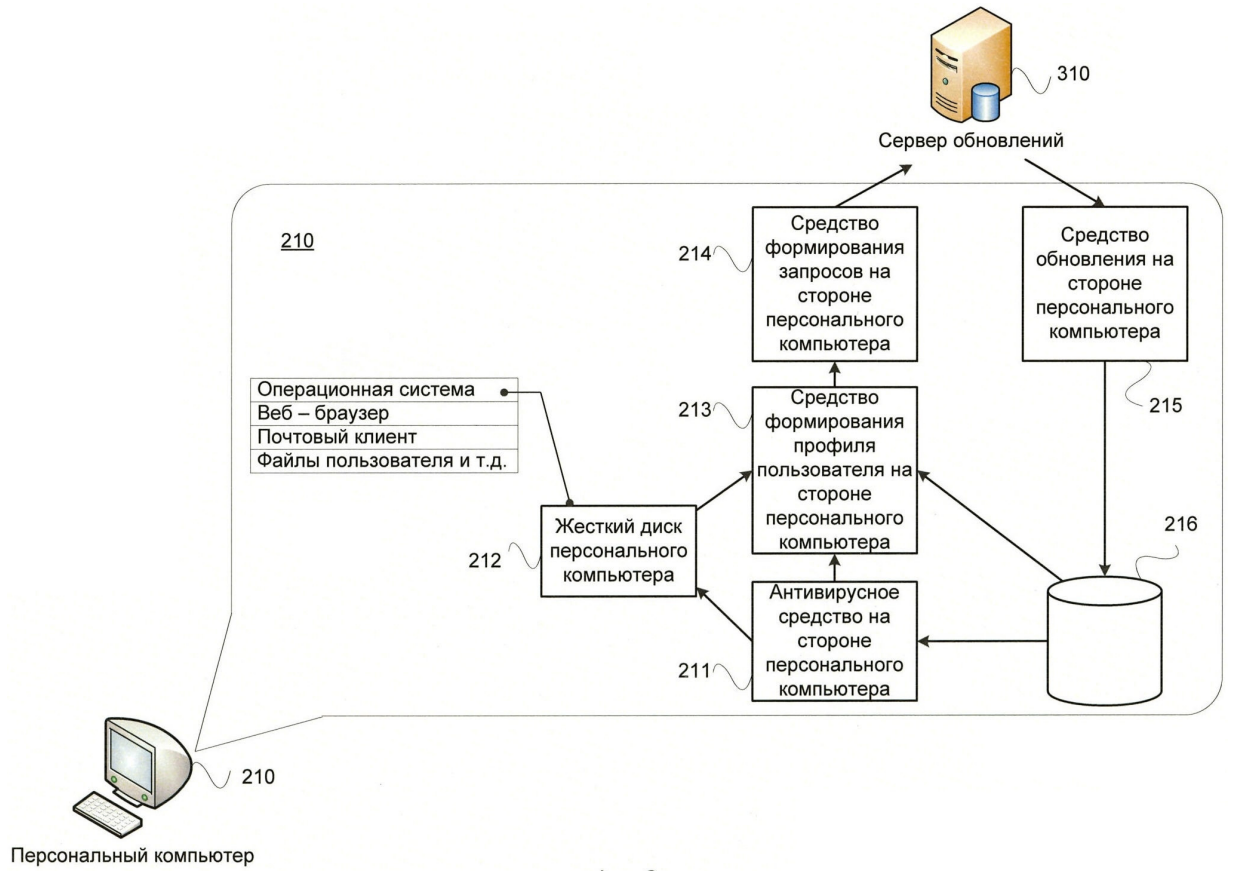
10. Способ по п.8, в котором производят внеочередной запуск средства обработки данных на стороне сервера обновлений с целью принудительного

обновления антивирусной базы данных на стороне персонального компьютера после обновления центральной антивирусной базы данных на стороне сервера обновлений при помощи средства принудительного обновления на стороне сервера обновлений.

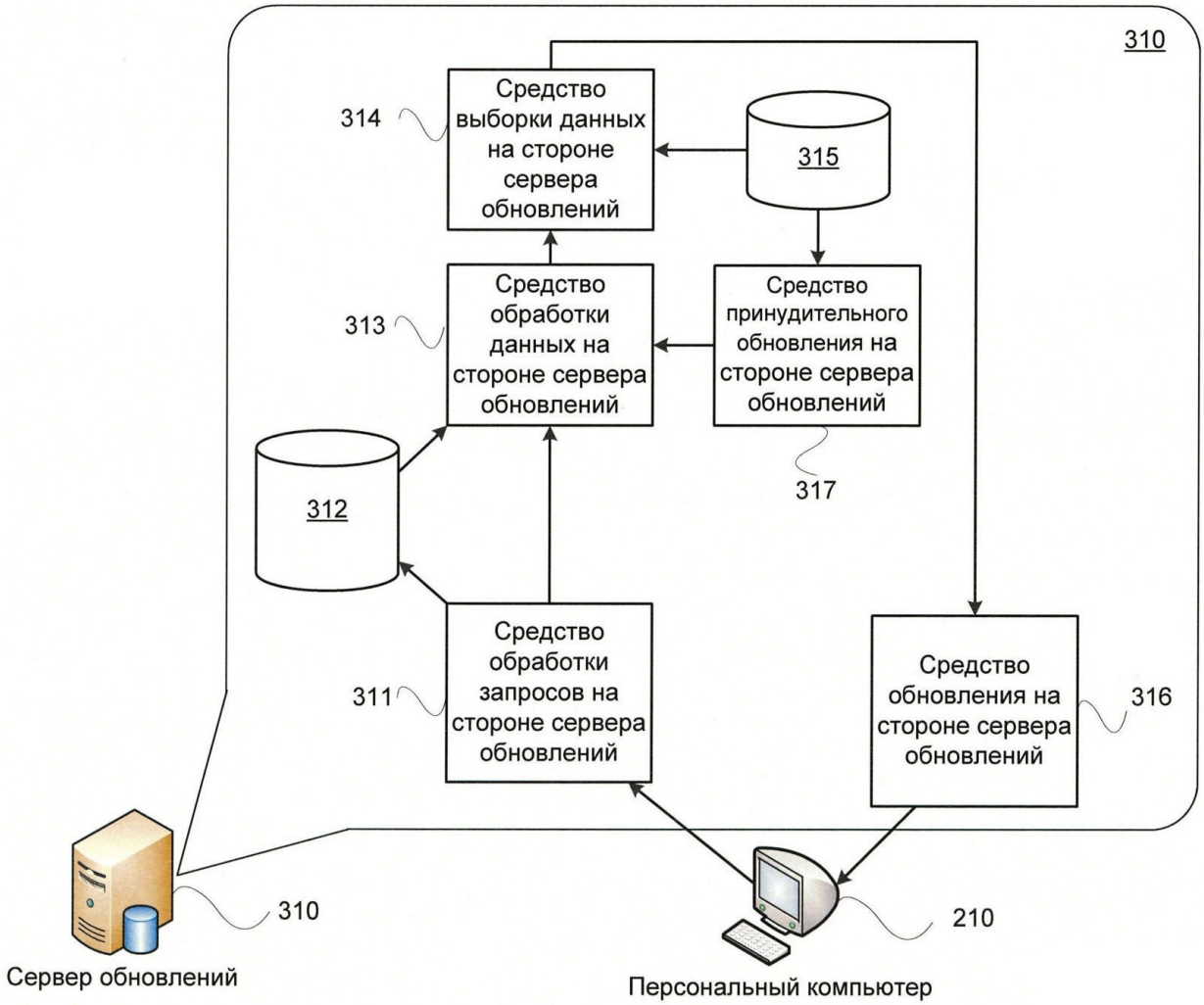
11. Способ по п.8, в котором средство формирования профиля пользователя на стороне персонального компьютера настраивают для получения только части данных антивирусной базы.


110
111
130
Интернет
120
122
125
126
128
121
123
124
127

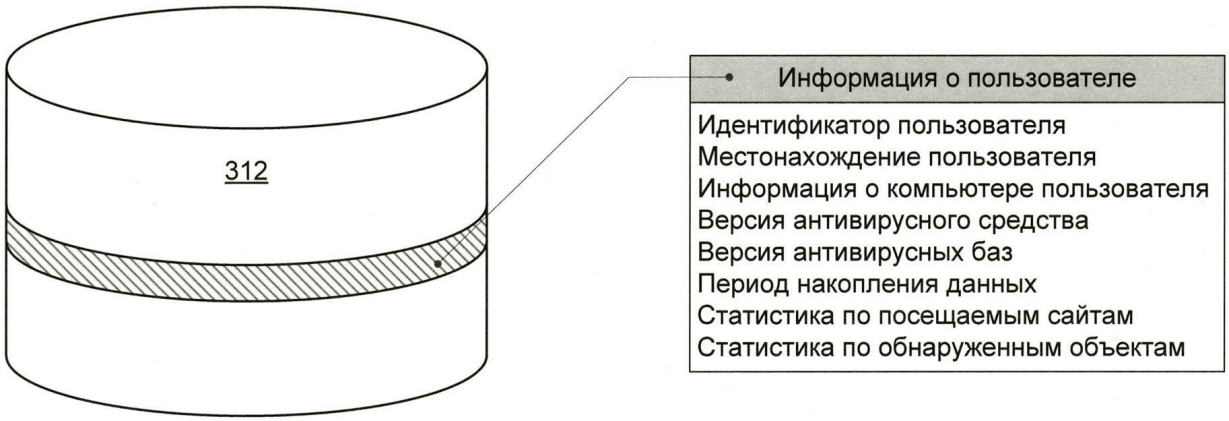
Фиг. 1


310
Сервер обновлений
210
214
Средство формирования запросов на стороне персонального компьютера
Средство обновления на стороне персонального компьютера
215
Операционная система
Веб – браузер
Почтовый клиент
Файлы пользователя и т.д.
213
Средство формирования профиля пользователя на стороне персонального компьютера
216
212
Жесткий диск персонального компьютера
Антивирусное средство на стороне персонального компьютера
211
210
Персональный компьютер

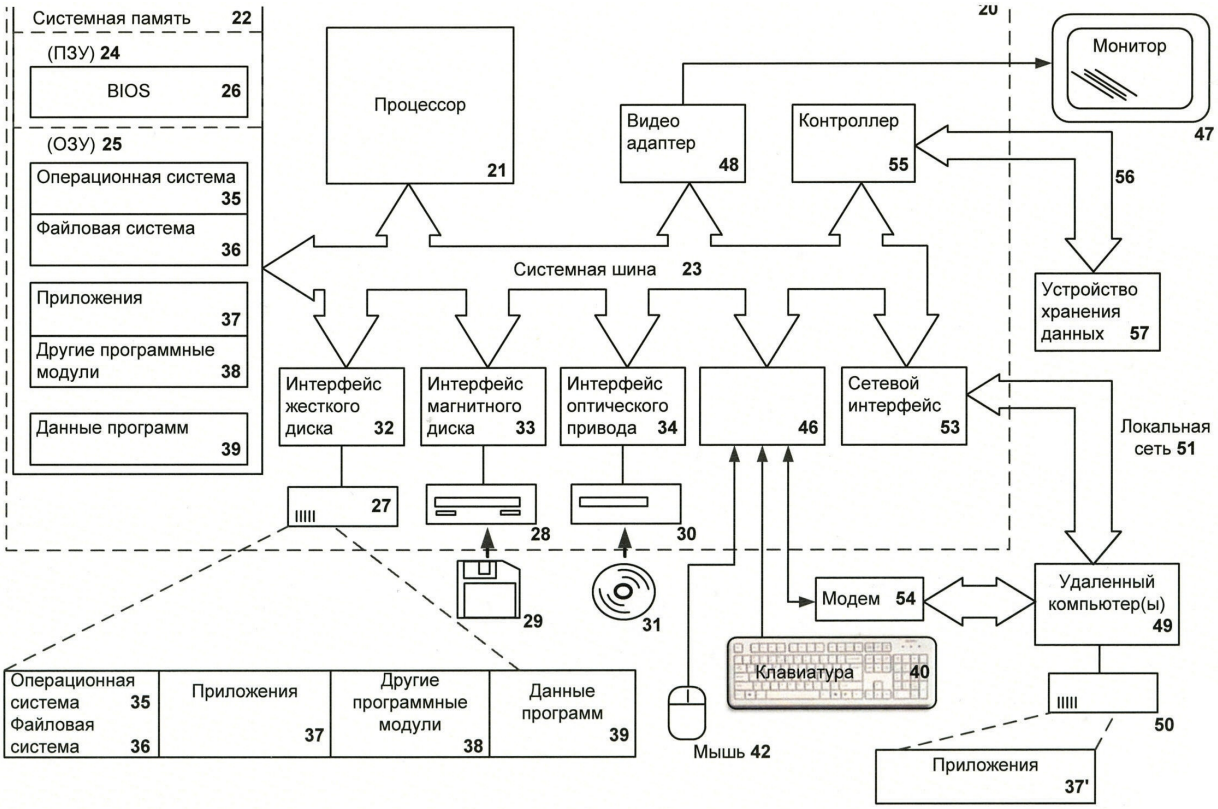
Фиг. 2


310
Средство выборки данных на стороне сервера обновлений
314
315
Средство обработки данных на стороне сервера обновлений
313
Средство принудительного обновления на стороне сервера обновлений
317
312
Средство обработки запросов на стороне сервера обновлений
311
Средство обновления на стороне сервера обновлений
316
310
Сервер обновлений
210
Персональный компьютер

Фиг. 3


312
Информация о пользователе
Идентификатор пользователя
Местонахождение пользователя
Информация о компьютере пользователя
Версия антивирусного средства
Версия антивирусных баз
Период накопления данных
Статистика по посещаемым сайтам
Статистика по обнаруженным объектам

Фиг. 4


Системная память 22
(ПЗУ) 24
BIOS 26
(ОЗУ) 25
Операционная система 35
Файловая система 36
Приложения 37
Другие программные модули 38
Данные программ 39
Процессор 21
Видео адаптер 48
Контроллер 55
Монитор
47
56
Системная шина 23
Устройство хранения данных 57
Интерфейс жесткого диска 32
Интерфейс магнитного диска 33
Интерфейс оптического привода 34
46
Сетевой интерфейс 53
Локальная сеть 51
27
28
30
29
31
Модем 54
Удаленный компьютер(ы) 49
Клавиатура 40
50
Мышь 42
Приложения 37'
Операционная система 35
Файловая система 36
Приложения 37
Другие программные модули 38
Данные программ 39

Фиг. 6